REMARKS

The Office Action dated April 11, 2005, has been carefully reviewed and the foregoing amendment is submitted in response thereto. New claims 27-36 have been added. Claims 1-12 and 21-36 are pending in the application.

The rejection of claims 1-4, 7-10, 21, and 24 under 35 USC 102(e) as being anticipated by Alegre et al is respectfully traversed. In the method and system of claims 1 and 7, an object associated with the Session ID is stored dynamically in a directory on a directory server coupled with the authorization server. The directory server permits other computer applications launched by the computer user to reference the Session ID on the user's computer. The user is authenticated and authorized to the first secured computer application to be launched by interacting with an authorization server. The user is authenticated and authorized to a second separately-secured computer application by accessing the object for the computer user on the directory server rather than requiring further interaction with the authorization server. The ability of additional applications to authenticate or authorize directly with the directory server achieves important advantages such as reducing network overhead.

MPEP §706.02 states that an invention is anticipated by a prior art reference under 35 USC §102 only if the prior art reference teaches every aspect of the claimed invention. Furthermore, in *Paperless Accounting, Inc. v. Bay Area Rapid Transit Sys.*, 804 F.2d 659, 665 (Fed. Cir 1986), the Federal Circuit stated that the "reference must sufficiently describe the claimed invention to have placed the public in possession of it."

Applicant respectfully points out that Alegre et al fails to teach all the claimed limitations, either expressly or implicitly. Alegre et al neither shows nor suggests separately-secured computer applications that are remotely launched by a user. Rather than authenticating and authorizing a user with respect to separately secured applications, Alegre et al creates a session key that is stored at a client browser and is used to access a trusted network. Whenever the user accesses the trusted network during the session, the session key must be transmitted with the access

request (col. 3, line 67, to col. 4, line 7). Thus, user authentication is checked for each and every individual remote access request by the user. The session key must be transmitted and checked with every incoming access request from the user, resulting in very high network overhead which is avoided by the present invention.

Alegre et al has no teaching whatsoever of multiple applications that each requires its own separate authorization. Therefore, there is likewise no teaching of using a directory to store an object accessed by more than one application for purposes of authentication. Claims 1 and 7 have been amended to even more distinctly claim that the computer applications are separately secured and that the second separately-secured application reads the Session ID, which allows the second application to locate the object on the directory server when authenticating and authorizing the second application. The session key of Alegre et al is always read and processed in the same way by the access server and not by any secured applications themselves. Therefore, claims 1-4, 7-10, 21, and 24 are allowable over Alegre et al.

The rejection of claims 5, 6, 11, and 12 under 35 USC 103(a) as being unpatentable over Alegre et al in view of Hartman et al is respectfully traversed. Hartman fails to correct for the deficiencies in Alegre. Therefore, claims 5, 6, 11, and 12 are allowable.

The rejection of claims 22, 23, 25, and 26 under 35 USC 103(a) as being unpatentable over Alegre et al in view of Blanco et al is respectfully traversed. Blanco et al does not use LDAP or X.500 to access objects having the limitations recited in the present claims. Thus, Blanco et al fails to correct for the deficiencies in Alegre et al, and claims 22, 23, 25, and 26 are allowable.

New claims 27-36 likewise define patentable subject matter over the cited references. They recite separately-secured computer applications that are remotely launched by the user. When launching a first application, the user is authenticated and authorized by exchanging security information between the user and an authorization server. When launching a second application, the user is authenticated and authorized by exchanging the stored security information between the directory server and the application server. None of the cited references either teach or suggest such a

combination.

In view of the foregoing amendment and remarks, claims 1-12 and 21-36 are respectfully submitted to be in condition for allowance. Favorable action is respectfully solicited.

Respectfully submitted,

Mark L. Mollon
Attorney for Applicant(s)
Reg. No. 31,123

Dated: June 14, 2005
MacMillan, Sobanski & Todd, LLC
One Maritime Plaza, Fourth Floor
720 Water Street
Toledo, Ohio 43604
(734) 542-0900
(734) 542-9569 (fax)